

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

VERSION RÉVISÉE

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
13 octobre 2005 (13.10.2005)

PCT

(10) Numéro de publication internationale
WO 2005/096135 A2

(51) Classification internationale des brevets⁷ : **G06F 7/52**

(21) Numéro de la demande internationale :
PCT/FR2005/000443

(22) Date de dépôt international :
24 février 2005 (24.02.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0402146 2 mars 2004 (02.03.2004) FR

(71) Déposant (*pour tous les États désignés sauf US*) :
FRANCE TELECOM [FR/FR]; 6, place d'Alleray,
F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (*pour US seulement*) : **GIRAULT, Marc** [FR/FR]; 4, rue Viviane, F-14000 Caen (FR).
LEFRANC, David [FR/FR]; Résidence Stéphanolyse, 7,
rue des Tilleuls, F-14000 Caen (FR).

(74) Mandataires : **LOISEL, Bertrand** etc.; Cabinet Plasser-
aud, 65/67, rue de la Victoire, F-75440 Paris Cedex 09
(FR).

(81) États désignés (*sauf indication contraire, pour tout titre de
protection nationale disponible*) : AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,
CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG,

KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,
MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,
PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,
ZW.

(84) États désignés (*sauf indication contraire, pour tout titre
de protection régionale disponible*) : ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO,
SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN,
GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US
seulement*

Publiée :

— *avec déclaration selon l'article 17.2)a); sans abrégé; titre
non vérifié par l'administration chargée de la recherche
internationale*

(48) Date de publication de la présente version révisée:
8 décembre 2005

(15) Renseignements relatifs à la correction:
voir la Gazette du PCT n° 49/2005 du 8 décembre 2005,
Section II

*En ce qui concerne les codes à deux lettres et autres abrégia-
tions, se référer aux "Notes explicatives relatives aux codes et
abréviations" figurant au début de chaque numéro ordinaire de
la Gazette du PCT.*

(54) Title: METHOD AND DEVICE FOR PERFORMING A CRYPTOGRAPHIC OPERATION

(54) Titre : PROCEDE ET DISPOSITIF POUR ACCOMPLIR UNE OPERATION CRYPTOGRAPHIQUE

(57) Abstract:

(57) Abrégé :



WO 2005/096135 A2

PATENT COOPERATION TREATY

PCT

DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT

(PCT Article 17(2)(a), Rules 13^{ter}.1(c) and 39)

Applicant's or agent's file reference BCT050021/EN	IMPORTANT DECLARATION	Date of mailing (day/month/year) 23/09/2005
International application No. PCT/FR2005/000443	International filing date (day/month/year) 24/02/2005	(Earliest) Priority Date (day/month/year) 02/03/2004
International Patent Classification (IPC) or both national classification and IPC G06F7/52		
Applicant FRANCE TELECOM		


This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below.

1. ☐ The subject matter of the international application relates to:
 - a. ☐ scientific theories.
 - b. ☐ mathematical theories.
 - c. ☐ plant varieties.
 - d. ☐ animal varieties.
 - e. ☐ essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
 - f. ☐ schemes, rules or methods of doing business.
 - g. ☐ schemes, rules or methods of performing purely mental acts.
 - h. ☐ schemes, rules or methods of playing games.
 - i. ☐ methods for treatment of the human body by surgery or therapy.
 - j. ☐ methods for treatment of the animal body by surgery or therapy.
 - k. ☐ diagnostic methods practised on the human or animal body.
 - l. ☐ mere presentations of information.
 - m. ☐ computer programs for which this International Searching Authority is not equipped to search prior art.
2. ☒ The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:

☒ the description
☒ the claims
☐ the drawings
3. ☐ The failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions prevents a meaningful search from being carried out:

☐ the written form has not been furnished or does not comply with the standard.
 ☐ the computer readable form has not been furnished or does not comply with the standard.
4. Further comments:

See supplemental sheet

Name and mailing address of the ISA/  Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer <p style="text-align: center; margin-top: 10px;">Iveta Bujanska</p> Telephone No.
--	---

FURTHER INFORMATION FROM PCT/ISA/203

The invention is not disclosed in a manner sufficiently clear and complete to allow it to be carried out by a person skilled in the art.

The description does not disclose the invention in terms that allow a proper understanding of the technical problem or its solution, and it does not give details of at least one embodiment of the invention.

The solution to the problem specified at page 3 lines 26 to 30 ("authentication using a public key in a hardwired logic chip") does not show how to calculate the value X, which is used in the essential phase 2 (figure 1) of the authentication procedure.

Furthermore, a person skilled in the art would not be able to apply the final essential verification phase because the application fails to provide any details of this phase. Without verification it is not clear how the technical problem is solved, and it is not possible to carry out a meaningful search of the prior art.

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (PCT Rule 66.1(e)). The applicant is advised that it is not normally the policy of the EPO in its capacity as International Preliminary Examining Authority to carry out a preliminary examination for subject matter that has not been searched. This applies whether or not the claims were amended after receipt of the search report or in the course of the procedure under PCT Chapter II. The applicant is reminded that if the application proceeds to the regional phase before the EPO an additional search may be carried out in the course of the examination (cf. EPO Guidelines, Part C, VI, 8.5) on the condition that the problems that led to the declaration under PCT Article 17(2) have been resolved.

TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

PCT

DECLARATION DE NON-ETABLISSEMENT DU RAPPORT DE RECHERCHE INTERNATIONALE

(article 17.2)a), règles 13ter.1.c) et 39 du PCT)

Référence du dossier du déposant ou du mandataire BCT050021/EN	DECLARATION IMPORTANTE	Date d'expédition(jour/mois/année) 23/09/2005
Demande internationale no. PCT/FR2005/000443	Date du dépôt international(jour/mois/année) 24/02/2005	Date de priorité (la plus ancienne) (jour/mois/année) 02/03/2004
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G06F7/52		
Déposant FRANCE TELECOM		


L'administration chargée de la recherche internationale déclare, conformément à l'article 17.2)a), qu'il ne sera pas établi de rapport de recherche internationale au sujet de la demande internationale pour les motifs indiqués ci-dessous.

1. ☐ L'objet de la demande internationale a trait à:
 - a. ☐ des théories scientifiques.
 - b. ☐ des théories mathématiques.
 - c. ☐ des variétés végétales.
 - d. ☐ des races animales.
 - e. ☐ des procédés essentiellement biologiques d'obtention de végétaux ou d'animaux, autres que des procédés microbiologiques et des produits obtenus par ces procédés.
 - f. ☐ des plans, principes ou méthodes dans le domaine des activités économiques.
 - g. ☐ des plans, principes ou méthodes dans l'exercice d'activités purement intellectuelles.
 - h. ☐ des plans, principes ou méthodes en matière de jeu.
 - i. ☐ des méthodes de traitement chirurgical ou thérapeutique du corps humain.
 - j. ☐ des méthodes de traitement chirurgical ou thérapeutique du corps animal.
 - k. ☐ des méthodes de diagnostic appliquées au corps humain ou animal.
 - l. ☐ de simples présentations d'information.
 - m. ☐ des programmes d'ordinateur pour lesquels l'administration chargée de la recherche internationale n'est pas outillée pour procéder à des recherches sur l'état de la technique.
2. ☒ Les parties suivantes de la demande internationale ne remplissent pas les conditions prescrites, de sorte qu'il n'est pas possible d'effectuer une recherche significative:

☒ la description
☒ les revendications
☐ les dessins
3. ☐ Le listage des séquences de nucléotides ou d'acides aminés n'est pas conforme à la norme prévue dans l'annexe C des instructions administratives, de sorte qu'il n'est pas possible d'effectuer une recherche significative :

☐ le listage présenté par écrit n'a pas été fourni ou n'est pas conforme à la norme.
 ☐ le listage sous forme déchiffrable par ordinateur n'a pas été fourni ou n'est pas conforme à la norme.
4. ☐ Les tableaux relatifs au listage des séquences de nucléotides ou d'acides aminés ne sont pas conformes aux exigences techniques prévues dans l'annexe C-bis des instructions administratives, de sorte qu'il n'est pas possible d'effectuer une recherche significative :

☐ les tableaux présentés par écrit n'ont pas été fournis.
 ☐ les tableaux sous forme déchiffrable par ordinateur n'ont pas été fournis ou ne sont pas conformes à la norme.
5. Observations complémentaires: voir les notes sur la feuille d'accompagnement

Nom et adresse postale de l'administration chargée de la recherche internationale  Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fonctionnaire autorisé Iveta Bujanska
---	--

SUITE DES RENSEIGNEMENTS INDICUES SUR PCT/ISA/ 203

L'invention n'est pas exposée de façon suffisamment claire et complète pour qu'un homme du métier puisse l'exécuter.

La description n'expose pas l'invention en des termes permettant la compréhension du problème technique et celle de la solution de ce problème,

et elle ne d'indique pas en détail au moins un mode de réalisation de l'invention.

La solution du problème définit dans la description en page 3, ligne 26 à 30, "authentification à clé publique dans une puce à logique câblée", manque des détails au sujet du calcul de la valeur X qui est utilisée dans la phase essentielle 2 (Fig. 1) de la procédure pour l'authentification.

En outre, l'homme de métier ne serait pas en mesure de mettre en application la phase finale essentielle de la vérification, puisque la demande ne fournit aucun détail concernant cette phase. Sans vérification, il n'est pas clair comment le problème technique est résolu, et une recherche significative sur l'état de la technique ne peut être effectuée.

L'attention du déposant est attirée sur le fait que les revendications ayant trait aux inventions pour lesquelles aucun rapport de recherche n'a été établi ne peuvent faire obligatoirement l'objet d'un rapport préliminaire d'examen (Règle 66.1(e) PCT).

Le déposant est averti que la ligne de conduite adoptée par l'OEB agissant en qualité d'administration chargée de l'examen préliminaire international est, normalement, de ne pas procéder à un examen préliminaire sur un sujet n'ayant pas fait l'objet d'une recherche. Cette attitude restera inchangée, indépendamment du fait que les revendications aient ou n'aient pas été modifiées, soit après la réception du rapport de recherche, soit pendant une quelconque procédure sous le Chapitre II.

Si la demande devait être poursuivie dans la phase régionale devant l'OEB, il est rappelé au déposant qu'une recherche pourrait être effectuée durant la procédure d'examen devant l'OEB (voir Directive OEB C-VI, 8.5) à condition que les problèmes ayant conduit à la déclaration conformément à l'Article 17(2) PCT aient été résolus.